EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ŠTUDIJA PRIMERA

NAČRT VARNOSTNIH UKREPOV

NAMEN

- prikazati, kako se **načrt varnostnih ukrepov uporabi v praksi**

- povezati:
  - oceno tveganj
  - določanje obsega ukrepov
  - izbiro in prioritizacijo ukrepov
  - prikazati vlogo vodstva in sistema vodenja

Primeri so poenostavljeni.

OPIS ORGANIZACIJE

Opis organizacije (primer)

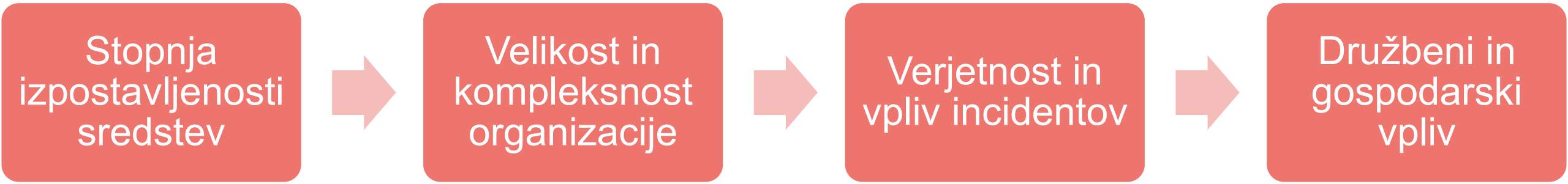
- srednje velika organizacija
- obdelava osebnih in poslovno kritičnih podatkov
- informacijski sistemi podpirajo ključne storitve
- zavezanost ZInfV-1

Izhodišča

ocena tveganj pokaže:

- tveganja človeškega faktorja
- tveganja nepooblaščenih dostopov
- tveganja izgube razpoložljivosti

KAKO DOLOČIMO OBSEG VARNOSTNIH UKREPOV



IZBOR VRSTE UKREPOV

Vrsta ukrepa	Opis	Primer
Organizacijski	Urejajo pravila, odgovornosti, postopke in upravljanje varnosti	Politike, usposabljanja, pogodbene zahteve, SOC
Tehnični (logično-tehnični)	Tehnološko tehnične rešitve, ki ščitijo sisteme	MFA, EDR, segmentacija, šifriranje
Operativni	Vsakodnevno izvajanje varnostnih postopkov in nadzora	Preverjanje varnostnih kopij, preverjanje delovanja varnostnih rešitev
Fizični in okoljski	Varujejo prostore, opremo in infrastrukturo pred fizičnimi grožnjami	nadzor dostopa do prostorov, UPS, zaščita kablovja

PRIMER POVEZAVE MED TVEGANJI IN VARNOSTNIMI UKREPI

Tveganje	Ukrep	Vrsta ukrepa
Izsiljevalska programska oprema (ang. Ransomware)	Offline backup + EDR + MFA	Tehnični
Nepooblaščen dostop do podatkov	RBAC (dodeljevanje dostopov glede na vlogo)	Organizacijski/tehnični
Izpad aplikacije	Nadzor diskovnih kapacitet	Operativni
Človeška napaka	Ozaveščanje + simulacija spletnega ribarjenja (mock phishing)	Organizacijski

PRIMERI PODROČIJ IN VRST VARNOSTNIH UKREPOV

Področje varnostnih ukrepov	Primeri ukrepov
Organizacijski ukrepi	Politika informacijske varnosti, politike gesel in sprejemljive rabe, klasifikacija podatkov, opredelitev vlog in odgovornosti
Upravljanje tveganj	Register tveganj, periodična ocena tveganj, ocena tveganj dobavne verige
Upravljanje dostopov (IAM)	MFA, RBAC, načelo najmanjših privilegijev, redni pregledi dostopov
Zaznavanje in spremljanje varnostnih dogodkov	Beleženje dogodkov, SIEM, opozorila in alarmi
Omrežna varnost	Segmentacija omrežja, požarni zidovi, VPN, zaščita brezžičnih omrežij
Zaščita naprav	Zaščita pred zlonamerno kodo / EDR, nadzor končnih naprav
Varnostno kopiranje in obnova delovanja	Varnostne kopije, testiranje obnovitve, opredeljeni RTO/RPO
Odzivanje na incidente	Načrt odzivanja na incidente, poročanje, sodelovanje s SI-CERT
Neprekinjeno poslovanje	BCP/DRP, analiza vpliva na poslovanje (BIA)
Dobavna veriga	Varnostne zahteve v pogodbah, ocenjevanje dobaviteljev
Fizična varnost	Nadzor fizičnega dostopa, varovanje prostorov, neprekinjeno napajanje
Usposabljanje	Ozaveščanje zaposlenih, simulacije napadov spletnega ribarjenja (mock phishing)
Skladnost in nadzor	Notranje presoje, spremljanje izvajanja politik

VLOGA VODSTVA

Izhodišče

Po izvedeni oceni tveganj in pregledu stanja:

- zaznano je **povečano tveganje napadov ribarjenja (phishing)**
- obstoječi ukrepi so **neenakomerno izvajani**
- presoja učinkovitosti kaže **pomanjkljiv učinek**

Odločitev vodstva

Vodstvo v primeru sprejme naslednje odločitve:

- potrdi **načrt varnostnih ukrepov**
- odobri sredstva za:
  - ciljno usposabljanje zaposlenih
  - dodatne tehnične kontrole (npr. MFA)
- določi **nosilce odgovornosti**
- zahteva **periodično poročanje** o učinkovitosti

Kaj se zgodi, če vodstvo ne ukrepa

Če vodstvo ne ukrepa:

- ukrepi ostanejo **na papirju**
- ni jasnih prioritet
- poročila nimajo vpliva
- tveganja ostajajo nespremenjena

Vloga vodstva

V tem primeru aktivna vloga vodstva omogoči:

- usklajeno izvajanje ukrepov
- jasno odgovornost
- merljivo izboljšanje učinkovitosti
- povezavo varnosti s poslovnimi cilji

IZBIRA IN PRIORITIZACIJA VARNOSTNIH UKREPOV

Izhodišče

Na podlagi:

- ocene tveganj
- potrjenega načrta varnostnih ukrepov
- omejenih virov (čas, denar, ljudje)

ima organizacija identificirane **3 prednostne ukrepe**:

1. uvedba večfaktorske avtentikacije (MFA)
2. nadgradnja programa ozaveščanja zaposlenih
3. izboljšanje nadzora nad privilegiranimi dostopi

Analiza možnosti

Možnost A – MFA

- takojšnje zmanjšanje tveganja zlorabe poverilnic
- vpliv na uporabniško izkušnjo
- zahteva tehnično uvedbo

Možnost B – Ozaveščanje

- dolgoročen učinek
- nizki stroški
- ne odpravi tehničnih ranljivosti

Možnost C – Privilegirani dostopi

- zmanjšanje vpliva incidentov
- manj viden ukrep
- več organizacijskih sprememb

Odločitev

Karikiramo, da se v tem primeru vodstvo odloči:

- **najprej MFA** (hitro zmanjšanje tveganja)
- vzporedno izboljšanje ozaveščanja
- privilegirani dostopi v drugi fazi

POVEZAVA TVEGANJ Z VARNOSTNIMI UKREPI (PRIMER)

ID tveganja	Opis tveganja	Stopnja tveganja	Ukrep ID	Naziv ukrepa	Prioriteta
R-001	Spletno ribarjene poverilnic (phishing)	Visoka	C-12	Zaščita + ozaveščanje	Visoka
R-002	Ransomware	Visoka	C-03	Varnostne kopije in obnova	Visoka
R-003	Neavtoriziran dostop	Srednja	C-02	MFA zaščita	Srednja
R-004	Izguba podatkov	Srednja	C-09	DLP zaščita podatkov	Srednja

ČLOVEŠKI FAKTOR

Izhodišče

Organizacija ima vzpostavljene naslednje ukrepe:

- letno obvezno usposabljanje zaposlenih
- podpis izjave o seznanjenosti z varnostnimi politikami
- navodila za prepoznavanje lažnih sporočil

Kljub temu:

- zaposleni še vedno klikajo na zlonamerne povezave
- poročanje incidentov je neenotno
- napake se **ponavljajo pri istih skupinah zaposlenih**

Ukrepi iz presoje

Presoja pokaže:

- usposabljanje je **preveč generično**
- vsebine niso prilagojene vlogam
- ni povezave med rezultati in dodatnimi ukrepi
- uspešnost se **ne spremlja sistematično**

Prilagoditev ukrepov

V tem primeru organizacija izvede:

- ciljno usposabljanje za rizične skupine
- krajše, pogostejše vsebine
- povezavo rezultatov simulacij ribarjenja z dodatnim ozaveščanjem
- jasen kanal za poročanje incidentov

VARNOSTNE KOPIJE IN OBNOVA

Izhodišče

Organizacija ima:

- vzpostavljen sistem varnostnih kopij
- dnevne avtomatske backupe
- dokumentiran postopek obnove

Kljub temu ob incidentu:

- obnova traja bistveno dlje od pričakovanj
- določeni sistemi niso vključeni v backup
- zadnje uspešno testiranje je bilo pred več kot letom dni

Incident

V organizaciji pride do:

- izpada ključnega informacijskega sistema
- začasne nedostopnosti podatkov
- pritiska poslovnih uporabnikov in vodstva

Vprašanje ni več, ali imamo varnostne kopije, ampak:

Ali lahko sistem dejansko obnovimo v sprejemljivem času?

Ugotovitve iz presoje

Presoja pokaže:

- RTO in RPO nista bila jasno opredeljena
- backupi niso redno testirani
- odgovornosti za obnovo niso jasno določene
- rezultati testiranj niso poročani vodstvu

Korektivni ukrepi

Na podlagi presoje organizacija izvede:

- jasno opredelitev RTO/RPO za ključne sisteme
- redno testiranje obnovljivosti (vsaj 1–2× letno)
- dokumentiranje rezultatov testov
- poročanje vodstvu o zmožnosti obnove

DNEVNIKI IN SLEDLJIVOST

Izhodišče

Organizacija ima:

- omogočeno beleženje dogodkov v informacijskih sistemih
- osnovne dnevnike dostopov in napak
- delno centralizirano hrambo dnevnikov

V praksi pa:

- dnevniki niso enotno zajeti
- hrambe niso časovno usklajene
- ni jasno, kdo dnevnike dejansko pregleduje

Incident

V organizaciji se zazna:

- sum nepooblaščenega dostopa
- nenavadna dejavnost uporabniškega računa
- zahteva vodstva po pojasnilu dogodkov

Ugotovitve iz presoje

Presoja pokaže:

- manjkajo dnevniki iz ključnih sistemov
- ni sinhronizacije časa
- dnevniki niso zaščiteni pred spremembami
- ni jasno opredeljene odgovornosti za pregled

Korektivni ukrepi

Na podlagi presoje organizacija izvede:

- centralizacijo dnevnikov za ključne sisteme
- sinhronizacijo časa (NTP)
- zaščito dnevnikov pred spremembami
- določitev odgovorne osebe za redne preglede
- dokumentiranje ugotovitev in poročanje

KAJ SMO VIDELI V PRIMERIH?

V primerih se je pokazalo, da:

- varnostni ukrepi **obstajajo**, a sami po sebi niso dovolj
- brez presoje učinkovitosti ukrepi **ne dajejo prave slike**
- brez načrta ukrepov presoja **nima operativnega učinka**
- odločilna je **vloga vodstva**

V praksi to pomeni

- Najprej organizacija ugotovi, **kje so tveganja**
- Na podlagi tega se odloči, **katere ukrepe bo uvedla**
- Ukrepe začne **dejansko izvajati**
- Nato preveri, **ali ti ukrepi res delujejo**
- Če ne, jih **prilagodi ali spremeni**

RAZMISLEK

- Koliko podrobno definiramo ukrepe?
- Kako določimo prioriteto pri uvajanju ukrepov?
- Kdo odloča o uvedbi ukrepov?
- Relacije mnogo-mnogo (sredstvo * tveganje * ukrep).
- Kompromis v trikotniku varnost-uporabnost-strošek.

HVALA ZA VAŠO POZORNOST

info@enisa.europa.eu

www.enisa.europa.eu